Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1. (CURRENTLY AMENDED) A method for evaluating a random number generator, the method comprising:

generating a stream of random numbers;

determining an average number of bits that have a value of a predetermined logic value at a predefined range of intervals using an exponential averaging operation (A); ~~and~~

determining whether the random number generator is ~~properly~~ providing random numbers that are sufficiently random by comparing an output of the exponential averaging operation to a predetermined acceptance range; and

providing a notification that the random number generator is not properly providing random numbers when the output of the exponential averaging operation falls outside the predetermined acceptance range.

2. (PREVIOUSLY PRESENTED) The method of claim 1, wherein the value of the predetermined logic value is one of 1 and 0.

3. (PREVIOUSLY PRESENTED) The method of claim 1, including determining that the random number generator is not properly providing random numbers when the output of the exponential averaging operation falls outside the predetermined acceptance range.

4. (CANCELED)

5. (PREVIOUSLY PRESENTED) The method of claim 1, including updating the exponential averaging operation each time a new bit is generated.

6. (CURRENTLY AMENDED) The method of claim 5, wherein the exponential averaging operation (A) is updated according to the following equation:

$A_{new} = \alpha \cdot A_{old} + b$,

wherein $\alpha = 1 - 1/n$, $n >> 1$, wherein n represents a number of bits and wherein b is a value of 1 when the predetermined logic value is obtained, otherwise 0.

7. (PREVIOUSLY PRESENTED) The method of claim 1, including generating a new set of random sequences when the output of the exponential averaging operation falls outside the predetermined acceptance range.

8. (PREVIOUSLY PRESENTED) The method of claim 6, wherein the predetermined acceptance range is defined as follows:

$[n/2 - c \cdot \sqrt{n}, n/2 + c \cdot \sqrt{n}]$,

where c is selected to achieve a desired security threshold level.

9. (CURRENTLY AMENDED) A method for evaluating a random number generator, the method comprising:

(a) generating a stream of random numbers of binary bits using the random number generator;

(b) determining an average number of bits that have a value of a predetermined logic value at a specific, predefined range of intervals using an exponential averaging operation (A);

(c) comparing an output of the exponential averaging operation to a predetermined acceptance range; ~~and~~

(d) determining that the random number generator is not generating random numbers that are sufficiently random ~~properly operating~~ when the output of the computed exponential averaging operation falls outside the predetermined acceptance range; and

(e) providing a notification that the random number generator is not properly operating when the output of the computed exponential averaging operation falls outside the predetermined acceptance range.

10. (PREVIOUSLY PRESENTED) The method of claim 9, including repeating (a) - (d) until the output of the exponential averaging operation repeatedly falls outside the predetermined acceptance range more than a predefined number of times.

11. (CANCELED)

12. (PREVIOUSLY PRESENTED) The method of claim 9, including generating a new set of random numbers when the output of the computed exponential averaging operation repeatedly falls outside the predetermined acceptance range more than a predefined number of times.

13. (CURRENTLY AMENDED) The method of claim 9, including updating the exponential averaging operation (A) according to the following equation:

$A_{new} = \alpha \cdot A_{old} + b$,

wherein $\alpha = 1 - 1/n$, $n >> 1$, wherein n represents a number of bits and wherein b is a value of 1 when the predetermined logic value is obtained, otherwise 0.

14. (PREVIOUSLY PRESENTED) The method of claim 13, wherein the predetermined acceptance range is defined as follows:

$[n/2 - c \cdot \sqrt{n}, n/2 + c \cdot \sqrt{n}]$,

where c is selected to achieve a desired security threshold level.

15. (PREVIOUSLY PRESENTED) An apparatus, comprising:

a random generator unit for generating sequences of binary bits;

a detector unit, coupled to an output of the random generator unit, for detecting whether the generated random sequences are unpredictable; and,

a switching unit, coupled to the output of the random generator unit and an output of the detector unit, for disabling the flow of the sequences when the generated random sequences are determined to be predictable,

wherein

the detector unit is configured to:

determine an average number of bits that have a value of a predetermined logic value at a specific, predefined range of intervals using an exponential averaging operation (A), and

determine that the sequence is predictable if the output of the exponential averaging operation (A) falls outside a predetermined acceptance range.

16. (PREVIOUSLY PRESENTED) The apparatus of claim 15, further comprising means for transmitting an alarm signal when the output of the exponential averaging operation falls outside the predetermined acceptance range.

17. (CURRENTLY AMENDED) The apparatus of claim 15, wherein the exponential averaging operation (A) is performed according to the following equation:

$A_{new} = \alpha \cdot A_{old} + b$,

wherein $\alpha = 1 - 1/n$, $n>>1$, wherein n represents a number of bits and wherein b is a value of 1 when the predetermined logic value is obtained, otherwise 0.

18. (PREVIOUSLY PRESENTED) The apparatus of claim 17, wherein the predetermined acceptance range is defined as follows:

$[n/2 - c \cdot \sqrt{n}, n/2 + c \cdot \sqrt{n}]$,

where c is selected to achieve a desired security threshold level.

19. (CURRENTLY AMENDED) A machine-readable medium having stored thereon data representing sequences of instructions, and the sequences of instructions which, when executed by a processor, cause the processor to:

generate a stream of random bits;

determine an average number of bits that have a value of a predetermined logic value at a specific, predefined range of intervals using an exponential averaging operation (A) on the number of bits indicative of the predetermined logic value;~~and~~

compare an output of the exponential averaging operations to a predetermined acceptance range; and

determine whether the generated random numbers are predictable in response to the comparison of the output of the exponential averaging operations to a predetermined acceptance range.

20. (PREVIOUSLY PRESENTED) The machine-readable medium of claim 19, wherein the generated random numbers are determined to be predictable when the computed exponential averaging operation falls outside the predetermined acceptance range.

21. (CURRENTLY AMENDED) The machine-readable medium of claim 19, wherein the exponential averaging operation (A) is performed according to the following equation:

$A_{new} = \alpha \cdot A_{old} + b,$

wherein $\alpha = 1 - 1/n$, $n>>1$, wherein n represents a number of bits and wherein b is a value of 1 when the predetermined logic value is obtained, otherwise 0.

22. (PREVIOUSLY PRESENTED) The machine-readable medium of claim 21, wherein the predetermined acceptance range is defined as follows:

$[n/2 - c \cdot \sqrt{n}, n/2 + c \cdot \sqrt{n}],$

where c is selected to achieve a desired security threshold level.

23. (NEW) The method of claim 1, including determining whether to utilize a random number from the stream of random numbers in an encryption application in response to the determination of whether the random number generator is providing random numbers that are sufficiently random.

24. (NEW) The method of claim 9, including determining whether to utilize a random number from the stream of random numbers in an encryption application in response to the determination of whether the random number generator is generating random numbers that are sufficiently random.